

**UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF TEXAS  
AUSTIN DIVISION**

<b>UNITED STATES OF AMERICA,</b>	§	
	§	
<b>Plaintiff,</b>	§	
	§	
<b>v.</b>	§	CRIMINAL NO. A-10-CR-297 LY
	§	
<b>DAVID ANDREW DIEHL,</b>	§	
	§	
<b>Defendant.</b>	§	
	§	

**UNITED STATES' RESPONSE IN OPPOSITION TO THE  
DEFENDANTS' MOTION AND FIRST SUPPLEMENTAL MOTION TO SUPPRESS  
SEARCH AND SEIZURE OF PHONE AND COMPUTER HARD DRIVES**

TO THE HONORABLE JUDGE OF SAID COURT:

The United States of America, by and through the United States Attorney for the Western District of Texas, files this response to the Defendant's Motion and First Supplemental Motion to Suppress (collectively referred to as the "Motion to Suppress Evidence") [Document Nos. 32 and 37 filed in this cause] filed herein.

I.

In his Motion to Suppress Evidence, the Defendant seeks to suppress the following fruits and evidence, including contraband and statements:

a. Evidence obtained from warrant issued on June 29, 2010 for: one Apple iPhone (32GB); one Seagate Barracuda 7200 250GB hard drive; and one Maxtor DiamondMax 21 500GB hard drive (the "Computer Warrant");

b. Evidence obtained from warrant issued on April 29, 2010, for a Yahoo! email account associated with the Defendant (the "Yahoo Warrant");

c. Evidence obtained from warrant issued on April 30, 2010, for a Gmail email account associated with the Defendant (the “Google Warrant”).<sup>1</sup>

The Defendant seeks to suppress this evidence by arguing that the Subject Warrants lacked probable cause for their issuance. He further argues that the good faith exception to the exclusionary rule recognized by United States v. Leon, 468 U.S. 897 (1984) does not apply because the magistrate judge’s determination of probable cause was not objectively reasonable.

## II.

Contrary to the Defendant’s assertions and arguments, the United States believes that the Subject Warrants were supported by probable cause; that the *Leon* good faith exception would apply to preclude the suppression of evidence obtained under any of the Subject Warrants found to lack probable cause; and that all evidence obtained from the execution of the Subject Warrants are not subject to suppression. Moreover, as discussed below, the Email Warrants were obtained under the authority of Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712, for which there is no suppression remedy under the SCA for violations thereof. Without addressing the Defendant’s assertions in detail, however, **the United States does not intend to introduce any evidence in its case-in-chief obtained as a result of the execution of the Subject Warrants.** In addition, no statements were obtained from the Defendant as a result of the execution of those warrants. The Motion to Suppress Evidence, thus, is moot.

Although the United States does not intend to introduce any evidence obtained from the Subject Warrants in its case-in-chief, even if the evidence obtained from the Subject Warrants was

---

<sup>1</sup> The Yahoo Warrant and Google Warrant may be collectively referred to as the “Email Warrants,” when appropriate. In addition, since the probable cause for each of these warrants was based on substantially identical facts, the warrants will be collectively referred to as the “Subject Warrants,” when appropriate.

otherwise subject to suppression, such evidence may be admissible under limited circumstances for impeachment of the Defendant or on rebuttal. *See, e.g., United States v. Havens*, 446 U.S. 620, 627-28 (1980) (impeachment of defendant).

### III.

Even so, the Email Warrants were issued under the authority of 18 U.S.C. § 2703(d), which is part of the Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712. Not only has the Defendant failed to note this critical point, the Defendant has made no assertion that the Email Warrants were issued in violation of the SCA. Although Section 2703(a) contemplates that disclosure of the content of an electronic communication by an electronic communication service be accomplished by “a warrant issued under the Federal Rules of Criminal Procedure . . .,” this provision only addresses the procedure for issuing the legal process required for disclosure of the content, not any remedy for any shortcomings of the warrant.

The Fourth Amendment generally does not protect materials in the possession of a third party from being obtained without a warrant, even where the owner of the materials maintains a reasonable expectation of privacy. *United States v. Miller*, 425 U.S. 435, 443 (1976). In addition, information in the possession of and accessible by a third party are subject to private searches that do not implicate the Fourth Amendment. *See, e.g., United States v. Jones*, 421 F.3d 359, 361-62 (5<sup>th</sup> Cir. 2005). Accordingly, as a matter of constitutional law, information and content sent through and/or stored by an ISP is likely obtainable without a warrant, and possibly without any legal process at all. Recognizing that privacy protections for such communications are desirable, Congress passed the Stored Communications Act to address the uncertain applicability of the Fourth Amendment to information in cyberspace and to extend *some* of those protections to electronic

communications and data. Section 2703 is part of the Stored Communications Act (SCA), which itself is part of the Electronic Communications Privacy Act of 1986 (ECPA).<sup>2</sup> The SCA imposes *by statute* the requirement of probable cause and a court order to obtain information and content from a third party provider. Consequently, a 2703(a) warrant is a creature of statute, not the Constitution.

Title 18, United States Code, Section 2703(a) specifically states that:

*A governmental entity may require the disclosure of the contents of a wire or electronic communication . . . only pursuant to a warrant **issued** using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent state warrant . . . .* [emphasis added].

Title 18, United States Code, Sections 2703(b)(1)(A) and 2703(c)(1)(A) also set forth identical language regarding “. . . a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent state warrant . . . .”

Although 18 U.S.C. § 2703 uses the term “warrant,” the warrant it authorizes is not a typical search and seizure warrant governed in all aspects by Federal Rule of Criminal Procedure 41. Instead, § 2703 envisions what is essentially a court order based upon probable cause that is subject only to certain procedures laid out in Rule 41.

The explicit language of Section 2703 indicates a 2703 warrant is subject only to the *issuance* procedures of Rule 41, i.e., Rules 41(b), (c), and (d). Although Rule 41 also has sections

---

<sup>2</sup> Courts and scholars have often used SCA and ECPA interchangeably, though such usage is probably inaccurate. While the SCA is codified at 18 U.S.C. §§ 2701-2712, ECPA also implemented changes to other statutes, such as the Wiretap Act.

addressing the execution and return of warrants, the SCA's statutory scheme does not apply those procedures to 2703 warrants. Indeed, one of the crucial differences between a 2703 warrant and a Rule 41 warrant is that the actual *execution* of a 2703 warrant is done entirely by the third party provider of electronic services rather than by a law enforcement officer. Law enforcement officers are not involved in searching or collecting the records and things subject to the order/warrant. 2703 warrants are typically e-mailed, faxed, or mailed to the provider and complied with solely by the provider. In essence, a 2703 warrant is a court order based on probable cause and directed to the provider to turn over records and information to law enforcement. In contrast, a Rule 41 search warrant is a court order based on probable cause directing a law enforcement officer to execute it and to search and seize the property designated. With a Rule 41 warrant, the person or entity in possession of the records and information at issue plays no role in the execution of the warrant, except to not interfere with the law enforcement agents conducting the search and seizure.

Federal courts have recognized that all aspects of Rule 41 were never meant to be applied to § 2703 warrants. Returning to the exact language employed in § 2703, these warrants are to be “issued using the procedures described in the Federal Rules of Criminal Procedure.” 18 U.S.C. § 2703(b)(1)(A). Relying on this language, the Seventh Circuit held that Rule 41(b) does not apply to § 2703 warrants because Rule 41(b) sets forth substantive, rather than procedural, requirements. *U.S. v. Berkos*, 543 F.3d 392, 397-98 (7th Cir. 2008). Other courts have supported this conclusion. *See In re U.S.*, --- F.Supp.2d ----, 2009 WL 3416240, at \*5 (D. Or. 2009) (“The plain language [of § 2703] thus specifies that only the procedures of Rule 41 are to be incorporated.”)<sup>3</sup>

---

<sup>3</sup> Although this case held, in part, that only the procedural requirements of Rule 41 applied to 2703 warrants, that conclusion seems to be broader than the express language of Section 2703. The court seemed to gloss over the fact that 2703 warrants are not executed according to the procedures set forth in Rule 41.

The law is unequivocal that the Stored Communications Act does not provide a suppression remedy for evidence obtained in violation of the SCA. *See* 18 U.S.C. § 2708 (“The [damages] remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.”); *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998) (“the Stored Communications Act expressly rules out exclusion as a remedy”); *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (“[S]uppression is not a remedy contemplated under the ECPA.”); *United States v. Hambrick*, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999) (“Congress did not provide for suppression where a party obtains stored data or transactional records in violation of the Act.”), *aff’d*, 225 F.3d 656, 2000 WL 1062039 (4th Cir. 2000); *United States v. Reyes*, 922 F. Supp. 818, 837-38 (S.D.N.Y. 1996) (“Exclusion of the evidence is not an available remedy for this violation of the ECPA. . . . The remedy for violation of [18 U.S.C. § 2701-11] lies in a civil action.”). Accordingly, even if the Email Warrants were obtained in violation of 18 U.S.C. § 2703(d) because the Applications failed to set forth probable cause, that argument cannot sustain a motion to suppress.

Accordingly, even if the Email Warrants violated the SCA – which the United States does not believe is the case – the evidence obtained pursuant to those warrants is not subject to suppression.

#### IV.

The Subject Warrants were supported by probable cause, as indicated by the totality of the circumstances. *Illinois v. Gates*, 462 U.S. 213 (1983). Although the Subject Warrants were supported by probable cause for their issuance, the court may address the applicability of the good faith exception without first deciding on the issue of probable cause. *Leon*, 468 U.S. at 923-24;

United States v. Sibley, 448 F.3d 754, 757-58 (5<sup>th</sup> Cir. 2006).

As to each of the Subject Warrants, the law enforcement agents reasonably relied on the Magistrate Judge's determination that the warrant was supported by probable cause. The affidavits supporting the warrants were lengthy (each were 43-47 pages in length), detailed, and not "bare-boned," and, among other things: provided a timeline of relevant facts and events showing the Defendant's long-term interest in and pursuit of unlawful sexual activity with minors, set forth relevant background regarding the characteristics and behaviors of child pornography collectors and producers, and included corroborating evidence and witness statements regarding the Defendant's child exploitation activities. The affidavits contain no deliberate or reckless false statements, nor has the Defendant alleged that any such statements were made. Accordingly, even if, for the sake of argument, probable cause were lacking – which the United States does not believe it is – the evidence obtained from the Subject Warrants are not suppressible because application of the good faith exception is warranted under the facts and circumstances.

V.

WHEREFORE, premises considered, the United States urges the Court to deny the Defendant's Motion to Suppress Evidence [Document Nos. 32 and 37 filed in this cause].

Respectfully submitted,

JOHN E. MURPHY  
United States Attorney

By: **/s/ Matthew Devlin**

---

MATTHEW B. DEVLIN  
Assistant United States Attorney  
816 Congress Avenue, Suite 1000  
Austin, Texas 78701  
(512) 916-5858  
Fax (512) 916-5854  
State Bar No. 00795012

**CERTIFICATE OF SERVICE**

I hereby certify that on October 19, 2010, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system which will send notification of such filing to the following:

Stephen M. Orr, Esq.  
804 Rio Grande Street  
Austin, Texas 78701  
(512) 472-8392  
Fax (512) 473-8417  
State Bar No. 15317000  
*Attorney for Defendant*

**/s/ Matthew Devlin**

---

MATTHEW B. DEVLIN  
Assistant United States Attorney



**UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF TEXAS  
AUSTIN DIVISION**

**UNITED STATES OF AMERICA,**

**Plaintiff,**

**v.**

**DAVID ANDREW DIEHL,**

**Defendant.**

§  
§  
§  
§  
§  
§  
§  
§  
§  
§

CRIMINAL NO. A-10-CR-297 LY

**ORDER**

Came on to be considered the Defendant's Motion and First Supplemental Motion to Suppress (collectively referred to as the "Motion to Suppress Evidence") [Document Nos. 32 and 37 filed in this cause], and the United States' response in opposition thereto, and the Court, having considered same, finds said motion lacks merit and should be denied. Accordingly,

**IT IS ORDERED** that the Defendant's Motion to Suppress Evidence be, and is hereby, DENIED.

**SIGNED** this \_\_\_\_\_ day of \_\_\_\_\_, 2010.

\_\_\_\_\_  
UNITED STATES DISTRICT JUDGE